TICOM/1-20

INTERROGATION OF SONDERFUEHRER DR. FRICKE OF OKW/CHI

(FORMERLY OF OKH/CHI).

The reports attached are of the first and second detailed interrogations of Sonderfeuhrer Dr. FRICKE at the OKM Signals School, FLENSBURG on 16th and 17th June, 1945.

Annexed to this report is the translation of seven pages of typescript. offered to the interrogators by Dr. FRICKE, being part of some sets of questions submitted to Chef WNV by unknown persons (presumably an Allied authority). These particular questions were passed on to FRICKE by WNV for preparation of answers. Question 5 of the second list and its answer are not FRICKE's.

The initial interrogation of Dr. FRICKE, together with Oberst KETTLER and Reg. Rat. Dr. HUETTENHAIN, all of OYW/Chi, and Oblt. SCHUBERT of OKH, were carried out in the SCHLOSS GLUCKSBURG on 15th June, 1945. A report on this interrogation is being issued separately.

TICOM 28th June, 1945.

Copy No. | No. of pages.

DISTRIBUTION

British
1. Director
2. D.D.3.
3. D.D.4.
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R) (2)
9. Col. Leatham

Ticom

10. Chairman.

11-12. S.A.C. (2)

13. Cdr. Bacon.

14. Cdr. Mackenzie.

15. Cdr. Tandy.

16. Lt. Col. Johnson.

17. Lajor Seaman.

18. Lt. Eachus

19. Lt. Vanco.

20. Capt. Cowan.

21. Lt. Fehl.

22-24. Ticom Files (3)

Additional Major G.W. Morgan A.D. (11ch).
L** CAr. Margar

Interregation of Somie funder Dr. Frions, wild at the Signal Second, Flensburg.

First Interrogation. 16 June 1945, P.M. Present: Major Secuen, AUS; Capt. Royffe, IC; Lt. Kirby, AUS

- Dr. Fricke was asked to give a chronological account of his career. He stated that he had been an astronomer at the Hamburg observatory. In 1954 he studied astronomy, mathematics and physics in Berlin. In 1955 he published his first astronomical works. These were critiques of studies made at the Mt Wilson observatories by Wilson and Hubble on the distribution of spiral nebulac. Later he studied cosmological problems under Prof. Milno in England. He published studies on the distribution and velocities of spirel nebulae in the German Astrophysical Journal. In 1939 he took his doctorate at the Göttingen observatory on the dynamics of stellar systems. He had obtained a scholarship at Edinburgh University which he was to have begun on 1 October 1939. He had got this scholarship through the good offices of Dr. MacVittic. On 1 May 1940 he wont to work at the Hamburg observatory, but was drafted into the Nachrichtentruppe during that year. On 15 May 1941 he was posted to OKH/Chi. At that time he knew nothing of cryptography. The director of the Hamburg observatory, Prof. HECKLINI, kept trying to get him back, to work on problems he had been occupied with before he was drafted, and which were related to the war effort: tables of air and ship navigation, and aerodynamic problems for airplane speeds over 1300 km per hr, as well as for rockets with speeds upwards of 3000 km per hr. These were purely mathematical problems involving the solution of differential equations which were farmed out to astronomical and mathematical institutions.
- it OKN/Chi he studied German cipher nethods and devised ne. oncs. These were military systems only. It was known that the single step. double box system TS 42 was breakable; they set out to solve the double stop system NS 42 ((double playfair)) and after a year's work found a schuler.

C /

The hold of his section at Olh/Chi at blis time is or. METSOF, the her about eight mathematicians under him. Prions a mind there until 1 devember 1944, at which time CH was forbidles to devise new system,

4. Returning to the subject of his work at on., Fricke state the no are for a year on the solution of Gorman systems, then set about the back of improvement. He had made some study of emily colution, but Dr. The end in a much letter informed on this subject. In 1941 they orificially india the and these were eliminated. They will not sown a contact . thum, but so that it oul? by come.

. In It is no developed the schlüsseltafel, or enciphering tables for 3/letter field codes. Fefore that they had been used without encipherment. Dilly

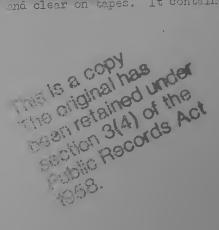
The original has under the original alaborithm alaborithm alaborithm act services act subjects.

6. Then he developed the masterschlussel. A study was made of the English cipher raster ((Cysquare)), and it was found to be very good. He doesn't know whether it was ever broken, but thinks not. However they thought that if the Germans used it in exactly the same form it would be broken because their messages were longer.

The there my rasters were ever solved, because although he was convinced to the properly used it was unbreakable, they never knew whether mistakes were more which rendered it soluble. We replied that it would be impossible for us to give him an answer. He said they always had wanted to work on their own to find just as they would do on foreign material, but were never given the coportunity. They never knew how the Army actually used the systems which they but out and they never saw any real traffic. When they asked for real traffic, they were given specially prepared messages, one of which read: "We are standing in borlin and see the Polish infantry coming down the Frankfurter Allce". They often reflected that the work on Russian systems showed that those systems were source if properly used, but if the cryptographers in Moscow could only see how they were used they would be very unhappy.

- 7. Whenever the Army was asked to change a system, there was a storm of protest. It was not they but the HNV (Heeresnachrichtenverbindung) staff which made the decision on methods to be used. The results depended on mother the officer at HNV at the time happened to know anything about cryptography. When the miles usually did not. In 1942 all hand systems were solvable. When the miles told this, the reply was that Germany had won all her battles so fir, using these systems, and there was no need to overload the troops with new mathods.
- 5. Dr. Pricke then proposed to speak of recent improvements in the enignementhing:
 - (a) Stecker Uhr. This is a small device to change the pluring. It gave 40 variations. They know that the strongth of the amenine lay in the stecker and therefore wish a to divide the install has per stecker by 40. The amenine was used only by the Laft of the woonly 1000 or so amenines for higher which as

- (b) Because of the uniform motion of the enigne, they con he rea that if messages of 600 or 700 letters were sent, they crude to order. If the instructions on maximum message length were followed, they know everything would be all right, but they felt cure that their important which were not followed. So they developed a new wheel with 26 notones which would be filled in as accired. These were called Lüchenfüllerwalze. They ished to avoid certain numbers of notones per wheel, and particularly consecutive notones, for with the latter it was difficult to predict the cycle except in special cases. Consequently they order that whoels should be used with one, five, seven, or nine notones only, and nover with consecutive notones. Some of these whoels were not ally built in Berlin by HETE SOETH & RINCKE, who built the enigne. They were to be produced in numbers by this form and by Siemens Halske, and were expected to be recay on 1 May 1945. They were not ready, however.
- (c) Pluggable reflector. This was used only on some Luftwaffe traffic. It is not considered important, as the stecker is the roll safeguard.
- (a) Gerat 39. This machine was to have embodied all their enignal experience. It would print both cipher and clear on tapes. It contained



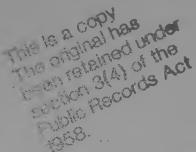
9. They saw that the americans had improved the Hagelin by introducing

This machine was used only by the Reichs etteraienst, which had a 10-aigit machine. As mess ges in depth are still soluble, they recently sought a means of changing the alphabet on the printing wheel.

10. The chief teleprinter cipher machines were the flemens STM T52c, a are a. They knew that models a and b, as well as c, could be broken, and this is vay they undertook to improve the machines. All of these machines performed first substitution, then a transposition, of the teleprinter-code latters. There is ten wheels with fixed patterns. These activated five relays which performed the substitution, and five others which performed the transposition, but the not aircotly connected. The relations but sen the were varied by means at place.

11. The rmy lawys sin that he teleprinter muchine could be solved. Then ONL/CLT proved that the 52c could be solved on 10,000 letters of text (this was done by Hittenhain and he could give the details), the Army sid well, nebody taps cur cables. This was probably false too, as they had reports of the Swedes reading t/p traffic, on the 52a used by their military attache in Stockholm. When these reports came in they are astounded because they could not break it themselves and doubted that anyone else could. They asked themselves whether the Swedes would really attempt to tap such difficult traffic, and if they did, how they could possibly have broken it. However they knew that all of their 52c and 52d keys had been captured in August/September 1944, and wondered if the Swedes had somehow got hold of these

12. He cent on to speak about the plugging.



13. Another type of t/p anothine they had observed in an American prototype.

14. The Auswartiges Amt used the T52 series of teleprinter cipher machine . The Luftwaffe had intended to drop the T52c on 1 May 1945.

15. He never saw the American machine referred to above. The Heereswaffer wat told then that we had once used this machine and then dropped it and they wondered why, inasmuch as we used the Hagelin, a simpler and well-known machine. In response to a question as to how the HWA knew about this machine, he said he did not know, but thought perhaps it was used commercially, as the Reichspost was said to have known about it too.

16. He then spoke about the FS Zusätze 40 and 42. These had recently been used only by the army. They performed a substitution only, and were used only on ./T.

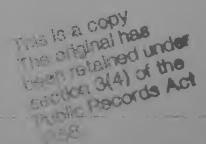
and in fact had under construction a 42c. He did not make the plans for this It was done by Dr LIEBTECHT, the expert on tale rinter cipher machines of theres afforcat. The makine would have his much improved synchronization, accomplished by means of quartz alcoks, and man, expected phic changes. I referred us to Hittenh in for these, as the latter had charge of it.

17. It has a constant to the state of the st

Second interrolation. 17 June 1945, P.i. Courlt Schubert as in the root but took no part in the discussion.

Present: - Major Lorgan I.C., Major Section a.U.S., Copt. Rayffe I.C., Lieut. Kirby A.U.S.

- 18. The question was raised of the place of the hearest from it in the Wehnmacht organization. Dr. Fricke stated that it was a succivision of the Wehnmacht organization. Dr. Fricke stated that it was a succivision of the Wells and Oberbefehl des Ersatzheeres ((reserve Hq)) which had charge of the Wells and Grupe of equipment for all arms and services. WA Pruf 7 developed Si had Grupe equipment, and Gruppe IV of this developed cipher machines. The head of the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. PLECHTER. The HUM itself was on the same level as the group was Oberstlt. The HUM itself was on the same level as the group was Oberstlt. The HUM itself was
- 19. He was asked the whereabouts of Dr. LIEBKNECHT of H.A, and replied the the last heard of him at Planken near Magdeburg, where the Versuchsanstalt des Heereswaffenants had been moved from Berlin.
- 20. Asked about the lain Reich Security office, which had been mentioned elsewhere in connection with cipher security ((possibly a misapprehension)), Fricke knew nothing about it. He referred to the RSHA generally, however, and said it had the same systems as the Army, at least the T52 machines and the enigma. He knew Oberinspektor Menzer, who had a development and security group like Fricke's, but who worked independently of him. Menzer made up systems for the RSHA, the Reichsbank, the Postoffice, and other governmental agencies. Menzer had been in OKW/Chi long before Fricke came and at one time had developed methods for the army. They worked in the same building. Menzer had recently been working on the development of two cipher devices, which he proceeded to describe.
- 21. The first was called Schlüsselkasten. It was under construction by the WANDERER typewriter firm at Chemnitz.



aevice weighed 800 grams.

-mis

22. The second device was similar but only the size of a conformation. The three cheels were mounted on the same axis, in the same plane as the box cover.

This device one coiled for Masselect isc. The coveragement of the transmit ended at the close of any term. If they had proved secure, the army had intermed to use them in place of its harm systems.

23. ((Previous information indicates, positive Prick and an error succession of CO/Oni Grappe II, a substitute III, assisting with city of the property. From a session that this section). Section III are not formal total the range of all fill excharge II as here, a postain of the range of the contract of the contrac

has, forestion, wie not arrive until a money or February 1949. We not no no look of crypto raphy, and had only a small staff from the Luftmaffe. The scotion accomplished nothing.

- 24. He was sheet that his section has a value of the intimal control or special theory of eigher pachine cycles. He said that it has not. One must have mathematical training for crypto raphy, but the mathematical training for crypto raphy, but the mathematical training for crypto raphy, but the mathematical training for example theory of probability ((!)). Skeet whether they had computed the period of 641, he is identified and the machine slightly, enough to see that the conversion of key into its complement as needed. Others worked on other security features of it. In fact, his section uid not develop the machine; hence aid most of it.
- 25. We said he had some things to add to the previous day's structures. He had neglected to mention venther systems. There was the Barbar schills el, a a terrible system used not for synoptics, but for reporting weither constants such as wind velocity at various heights: 100, 200, ... 10,000 meters, for the information of anti-aircraft and artillery. It employed an additive with as many as 100 messages in depth. Chef HEV had created it into as many as 100 messages in depth. Chef HEV had created it into use in 1939 and OfW/Chi never heard of it until 1944. In a day or two "I saw that it was clear text". He added that an enemy might think these messages unimportant, but in fact they agre extremely valuable and could even be used by enemy bombers for calculating the trajectory of their bombs. A new system had therefore been devised, and instructions printed, but it had not gone into effect. He was required to use an additive table of the same size, to save paper, so he are an eight-position grille, of which several were/to be used on the additive table during the month.
- 26. The synoptic systems used by the Reichsvetterdienst were also poor. It was therefore intended to introduce the S^G 41, on which cribs would be of no use. First they planned to use the machine in letter form, but liter they decided to have a digit model.
- 27. With regard to the instructions for making up emergency enigma kers thich he had given us, he wished to say that these were issued recently when a color transportation made it impossible to distribute new keys.
- 28. With regard to the tapping of their 52d lines, he haded that there had a nonly a few evidences of this. Nost came from Oberpostrat HALDER in the office of the mil. att. Stockholm, whose latest report thereof was received in Cept mar 1944. In consequence they put their newest and most secure machines, the Time and T43 onto this line. This same HALDER, however did a very foolish thing himself which OKW/Chi was at a loss to understand; he asked Calo to send him T52 keys in clear.

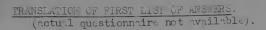
(0

- 29. With regard to SZ 40 and 42, he said he had asked that they be used only on Linieverkehr and not Netzverkehr, because two messages in depth could by read.
- 30. We then asked him to tell what he know of German ciphony. He sid not incomplement systems were actually in use. Lethods used were brocked, and amounted only to Erschwerungsgerat ((lit. 'device for making difficulty')). I fact he knew only of ordinary inverters (sor molers). How wer it was interested to build other types. They was developed by Prof. VIERLING, last known to at Fouristein, Franken. He worked with Dr LIEBLIECHT of the Heeres of fernal. They had developed two types, which he knows about only from a nversations with LIEBKIECHT.
- 31. The first was called 'Baultin'. It too was only in Fresh, run sger"t. It employed two principles: first the "userbeinischung, described is a superingusition of other frequencies on the natural frequencies of the voice treat, and accord an inverter. OFF/Chi as not directly concerned with the narrofficially told bout them. Virius people worked in this inaquadently. For example, Siemens worked independently of Vierling and Dielknacht. The term was in fact ready recently. He forgets which is not a production to have been by Vierling or by Biemens.
- 32. The sec number was allea 'nuenstliche aproch' ((rtificial aproch')) It out the frequency band vertically into seguents on a cipherea them separately, in a summer malurous to the ancipherment of the letter, by the SZ 40. He could give nevertils of the encipherment.

33. Ho had seen an American machine on the Tigerstedt principle taken from a Mustang. It had a magnetophone band which revolved between nine heads which scrambled the speech horizontally (i.e. in time). This type of machine was rejected in Germany because you had to wait in between utterances for the machine to act. He himself did not think 750 milliseconds was very long to wait, but he supposed if a German major was talking to a general, the latter would find it desirable to cut him off abruptly with a reply.

Asked about the Forschungsant, he said he knew none of those people until some of them came to Schloss Glucksburg. They had a bad name at OKW/Chi. Nothing was expected from them. He thought they were a big name with nothing behind it. When told that they employed 2,500 people he said, "For their deciphering they should have needed a handful. They must have had other work to do, but what the devil could they have been doing with 2,000 people?"

35. He said that Huttenhains' people had worked on the T52 solutions. He thought that he and Huttenhain' given sufficient time, and preferably with a captured machine to refer to, could work out the solution for us.



Wachrichtenstelle Thef WAV

Insacker 18/5/45

Ref.

Codes and Cyphers.

In connection with tell phone call by 2/Lt. ESC: of 18/5/45

To: Chief of Defence Force Signals Communications (in V)

In enswer to question 1)

The Dept. responsible for Codes and Cyphers is:

a) For the Army: Within the sphere of Chief of Defence Force Signals Communications (WNV)

b) For the Navy: Within the sphere of Supreme Command of the Navy.

c) For the Air Force: Within the sphere of the C. in C. of the Air Force Southern Sector.

In answer to question 2)

Cyphers for the army are prepared in approx. 25 printing works in the Central Germ my area. They are printed there and are distributed by the army High Command.

No information can be given as regards cypher preparation and distribution for the Navy and the Air Force.

Thomswer to question 3)

The senior officer is:

- a) For the Army: Lt.Col. LE TIG at present at General Eisenhower's G.H.W.
- b) For the Navy: Kapitaen our See LUCAN Naval supreme Command.
- c) For the Air Force: Lt. Col. SCHULZE. C. in C. of the Air Force Southern Sector.

In answer to question 4)

There are no longer any documents available for the ARMY; orders were issued to destroy them. Nothing is known here on the whereabouts of Naval or Air files.

In answer to question 5)

There is no longer available code or cypher information with Army authorities in the Northern +Sector, as they were destroyed in accord more with orders. No mare material is being prepared.

Three trucks of cypher material left in LLF/S.ALE in the middle of April to go to the Southern Sector; present wherehouts unknown. Equipment was administer a and distributed for the Army sphere by Army High Command/Signals Dept. (a. tsgrup a Nachrichten). Orders for such equipment were also issued by this authority. Nothing a m be said from here, therefore, as to whether equipment is lying in stock anywhere.

Nothing can be said an the above points concerning hir Force or Navy.

In enswer to question 6)

As for sive know here, there are no dumps for cypher and rid for the army. It is possible that there are still stocks left at the printers of cypher material, high his not yet been used. We know nothing about possible Mayor or air cymps. TRANSLATION OF STOOMS OF STOOMS ARE (Questions 3,4 and 5 and answers only vailable)

Question 3) Information on all Codes and Cyphers, including cypher anothines and books, used by German civil and military authorities in both Germany and the occupied territories and including exhaustive details on their hardling.

answer

1

Information can be given on the foll ling cypher processes (hand and machine cyphers), used by German military and wivil authorities in Germany and occupied territories.

I. Hand Cyphers

- Three letter codes with daily changing recypher by key tables. Three letter codes are books of limited scope, compiled by units themselves within the sphere of the Army and, in the Navy and Air Force, are issued by the Supreme Commans of these parts of the Defence Force. Recyphering tables were all delivered by the Supreme Commands.
- b) Raster cypher 44 Daily changing raster stencils, column and rod keys and conversion tables for encoding the keys. Used by Armay, Air Force, Public Authorities; in the Navy only in lateral traffic. In the Army it was also used as a met. key.
- c) Roster Replacement cypher and emergency cypher for it. Both are special double transpo, cyphers with squares blacked out in the columns of the first eages. Used by Army, Air Force and Public Authorities.
- d) Barbara Code Figure cards for encoding artillery et.
 reports for Army and Anti-aircraft artillery, principle of
 the encoding: Figures of the Barbara tables are added to
 the figures of the "clear" weather reports.
- e) Wenther substitution tables Figure cypher for encyphering met. reports in the Reich Weather Service. Principle of the encyphering: Figures of the clear met. reports are substituted by figures on the met. substitution tables.
- f) It is known that other hand keys were in use in the Navy and in the diplomatic service, but details are not known.

II. Machine Cyphers

- a) Stecker-Enigna with 3-wheels Used by Army, Air Force,
 Public Authorities. Daily changing key: order of wheels,
 tyre setting, stecker connections. Choice of 3 wheels from
 a set of 5. To some extent steckered auxiliary wheels are
 being made.
 Changing setting and key from message to message.
- b) Stecker-Enigna with 4 wheels Used by Navy, Daily changing keys as under (a). Choice of 4 wheels from a set of 8. Variable setting and key from message to message.
- c) Cormercial Enigna Archine with 4 wheels, no stockers. Used by Public Authorities.
- d) Cypher Machine 41 Hagelin chine with irregularly driven wheels. Used in Reich Leterrole ical Service as a figure machine. Not used as a letter ...chine.

III Teleprinter inchines

Type 52 c, c, e. - Cypher principle. Substitution and transposition of the impulses of the international T/T alphabet. The changes in the impulses are guided by 10

wheels with fixed lugs. The drive in ty e 52c is regular but with types 52d and e it is irregular. Daily changing keys. Type 52c used in line working, Types 52d and e in W/T and line working. Used by Army, Navy, Air Force and Public Authorities.

- b) Hachines 40 and 42. Principle: Substitution of the impulses of the international T/P alphabet directed by 12 wheels with variable lugs. Drive partly regular, partly irregular. Daily changing lugs as keys. Used in line and W/T working. Used by Army and Public Authorities.
- c) Teleprinter T 43. Principle: The symbols of the clear teleprint are encyphered by means of individual perforation strips. Used by Army, Navy, and Air Force. Detailed descriptions of the processes and their use are given in the instructions for working. There are no instructions available here.
- Guestion 4)

 A resume of all call-sign and cover-name systems used by Germany and/or her Allies in W/T and R/T, both in Civil and Military traffic of Germany and the other Allied countries.

Answer I. Call-sign Systems

- a) Haphazard choice of call-signs.
 Used by army and Air Force forward of Division. The Sigs
 Officer responsible at Division chooses call-signs
 independently.
- b) Call-sign Encyphering.

 Used by Army and Air Force rearwards of Division. Fixed basic call-signs are issued for lengthy periods in accordance with the Army Call-sign Book. Call-signs are changed by encyphering the basic call-sign with the call-sign key.

 The call-sign key itself is a substitution table for figures and letters.

 The Enigma machine key serves as an emergency key for encyphering call-signs, whereby the fixed basic call-signs are encyphered.
- c) The Naval call-sign systems and those of Public Authorities are not known here.

II. Cover-names and Camouflage devices.

Different cover-names and camouflage tables were issued by the 3 Services which at times were valid for considerable periods. These were not based on definite systems. In the Army, telephone traffic was camouflaged in accordance with the Army annual No.427 entitled, "Protection of Signals Communications".

Nothing is known here of the use in the Navy and air Force of cover-names and camouflage devices.

Guestion 5) Locations of all M/T, R/T and D/ stations used for en my signals purposes together with details of their organisation

.nswer W/T and R/T traffic were included in:

- I. The Wehrmacht Sigint stations to
 - a) LaUF
 - b) TREUMANIETZM

II. The fixed ray Sigint stations:-

- 1. (HUSUM)
- 2. (FUENSTER)

3. (EUSKIRCHEN!)

4. (STUTTGART/CAMETADT)

5. (GR.Z.)

6. (TALLY) ? TALLIN

7. (STRIEGAN)

8. (KUHNIGSBERG/PR.)

As regards operating and allocation of tasks, the Sigint stations were subordinate to;-

- I. Cryptographic office of the Chief of Wehrmacht Signals Communications at OKW;
- II. Head Sigint office with Chief of Army Signals matters at OKH.

The results were exploited at:-

- I. OYW/Chi,
- II. Chief of Arm, Signals Matters, Head Sigint Office.

Final r sults were reported to;-

- I. OKW. Ops. Staff.
- II. Coneral Staff of the Army, foreign armies West or East.
- III. There was one D/F station with each of the Vehracht or Fixed Sigint stations.